How Grades Were Assigned

The Committee's computer security grades are based on information contained in the Federal Information Security Management Act (FISMA) reports from agencies and Inspectors General (IG) for fiscal year 2004.

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is the FISMA. FISMA lays out the framework for annual IT security reviews, reporting and remediation planning at federal agencies. FISMA requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to the OMB in September of each year along with their budget submissions. FISMA also requires that agency heads report the results of those evaluations annually to the Congress and the Government Accountability Office.

On August 23, 2004, OMB provided final reporting guidance to agencies and IGs on implementing the provisions of FISMA. OMB instructed the agencies to submit reports summarizing the results of annual IT security reviews of systems and programs, agency progress on correcting identified weaknesses, and the results of IGs' independent evaluations. Similar to last year's guidance, agencies and IGs were required to use specific performance metrics in assessing and reporting the status of their agencies' security program.

Assignment of Grades

In assigning grades, the Committee followed the methodology developed for the fiscal year 2003 FISMA grades, with the exception of adjustments required by changes in OMB's FISMA reporting instructions (see below). This ensures consistency in the methodology used to assign grades and serves to highlight progress made by agencies.

The weighted scores are based on OMB's performance metrics, with a perfect score totaling 100 points. Since OMB provided a range of responses for most questions, the number of points assigned to each response is proportional to the extent the element has been implemented. For example, agencies received zero (0) points for a response indicating a percentage that falls below an acceptable threshold (for example: 50% or less of known IT security weaknesses being incorporated in the Plan of Action and Milestones). Proportionally, more points were given for answers that ranged between 51 and 70%, 81 and 95%, etc. The full weighted value was awarded for answers that ranged between 96 and 100%. For more specific weighting of questions see the scoring methodology.

Based on its analysis of the agency and the IG's responses, the Committee tallied the scores for the 24 agencies. The final numerical score is the basis for the agency's letter grade. Letter grades for the 24 major departments and agencies were assigned as follows:

90 to 93 = A-	94 to 96 = A	97 to 100 = A+
80 to 83 = B-	84 to 86 = B	87 to 89 = B+

70 to 73 = C-	74 to 76 = C	77 to 79 = C+
60 to 63 = D-	64 to 66 = D	67 to 69 = D+
59 and lower = F		

Major Changes to the Weighting of Grades

Changes in OMB's FISMA reporting instructions from FY03 to FY04 required the Committee to make several adjustments to the scoring. The major changes are listed below.

To facilitate future consistency, the Committee organized the scoring into the following major categories: Annual Testing, Plan of Action and Milestones, Certification and Accreditation, Configuration Management, Incident Detection and Response, Training and Systems Inventory. Changes for each area are listed below.

Annual Testing – No changes made.

Plan of Action and Milestones – No changes other than instructing agencies to report security weaknesses as significant deficiencies instead of material weaknesses.

Certification and Accreditation – OMB requested IGs to assess and report on their agency's Certification and Accreditation process. The IGs' response to this question determined whether an agency received full credit (if the IG approved of the process), one-half (if the IG found the process flawed), or none (if the IG declared the process poor) of the points awarded to the agency based on the reported number of systems certified and accredited.

Configuration Management – New performance metrics were added to this area in 2004. Agencies had to provide an evaluation of their policies in this area. Agencies also reported the number of systems that underwent vulnerability scans and penetration tests. This area is scored by deducting points either for a lack of configuration requirements for a system, or for low levels of implementation of existing requirements.

Incident Response and Detection – No changes made.

Training – No changes made.

Inventory – OMB requested that agencies report on the extent to which they have maintained and updated their inventory of systems. Agencies received no deduction from their final scores if their IG agreed with the CIO 96% of the time or higher on total inventory numbers; and, if their IG agrees that the agencies maintained their inventory of systems 96% of the time or higher. Otherwise, a full letter grade was deducted from their final score.